Article - State Government

[Previous][Next]

§10–1305.

(a) (1) In this section, "breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a unit.

(2) "Breach of the security of a system" does not include the good faith acquisition of personal information by an employee or agent of a unit for the purposes of the unit, provided that the personal information is not used or subject to further unauthorized disclosure.

(b) (1) If a unit that collects computerized data that includes personal information of an individual discovers or is notified of a breach of the security of a system, the unit shall conduct in good faith a reasonable and prompt investigation to determine whether the unauthorized acquisition of personal information of the individual has resulted in or is likely to result in the misuse of the information.

(2) (i) Except as provided in subparagraph (ii) of this paragraph, if after the investigation is concluded, the unit determines that the misuse of the individual's personal information has occurred or is likely to occur, the unit or the nonaffiliated third party, if authorized under a written contract or agreement with the unit, shall notify the individual of the breach.

(ii) Unless the unit or nonaffiliated third party knows that the encryption key has been broken, a unit or the nonaffiliated third party is not required to notify an individual under subparagraph (i) of this paragraph if:

1. the personal information of the individual was secured by encryption or redacted; and

2. the encryption key has not been compromised or disclosed.

(3) Except as provided in subsection (d) of this section, the notification required under paragraph (2) of this subsection shall be given as soon as reasonably practicable after the unit conducts the investigation required under paragraph (1) of this subsection.

(4) If, after the investigation required under paragraph (1) of this subsection is concluded, the unit determines that notification under paragraph (2) of

this subsection is not required, the unit shall maintain records that reflect its determination for 3 years after the determination is made.

(c) (1) A nonaffiliated third party that maintains computerized data that includes personal information provided by a unit shall notify the unit of a breach of the security of a system if the unauthorized acquisition of the individual's personal information has occurred or is likely to occur.

(2) Except as provided in subsection (d) of this section, the notification required under paragraph (1) of this subsection shall be given as soon as reasonably practicable after the nonaffiliated third party discovers or is notified of the breach of the security of a system.

(3) A nonaffiliated third party that is required to notify a unit of a breach of the security of a system under paragraph (1) of this subsection shall share with the unit information relating to the breach.

(d) (1) The notification required under subsection (b) of this section may be delayed:

(i) if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or

(ii) to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.

(2) If notification is delayed under paragraph (1)(i) of this subsection, notification shall be given as soon as reasonably practicable after the law enforcement agency determines that the notification will not impede a criminal investigation and will not jeopardize homeland or national security.

(e) The notification required under subsection (b) of this section may be given:

(1) by written notice sent to the most recent address of the individual in the records of the unit;

(2) by electronic mail to the most recent electronic mail address of the individual in the records of the unit if:

(i) the individual has expressly consented to receive electronic notice; or

(ii) the unit conducts its duties primarily through Internet account transactions or the Internet;

(3) by telephonic notice, to the most recent telephone number of the individual in the records of the unit; or

(4) by substitute notice as provided in subsection (f) of this section if:

(i) the unit demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of individuals to be notified exceeds 175,000; or

(ii) the unit does not have sufficient contact information to give notice in accordance with item (1), (2), or (3) of this subsection.

(f) Substitute notice under subsection (e)(4) of this section shall consist of:

(1) electronically mailing the notice to an individual entitled to notification under subsection (b) of this section if the unit has an electronic mail address for the individual to be notified;

(2) conspicuous posting of the notice on the website of the unit if the unit maintains a website; and

(3) notification to appropriate media.

(g) The notification required under subsection (b) of this section shall include:

(1) to the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;

(2) contact information for the unit making the notification, including the unit's address, telephone number, and toll–free telephone number if one is maintained;

(3) the toll–free telephone numbers and addresses for the major consumer reporting agencies; and

(4) (i) the toll–free telephone numbers, addresses, and website addresses for:

1. the Federal Trade Commission; and

2. the Office of the Attorney General; and

(ii) a statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft.

(h) (1) Before giving the notification required under subsection (b) of this section, a unit shall provide notice of a breach of the security of a system to the Office of the Attorney General.

(2) In addition to the notice required under paragraph (1) of this subsection, a unit, as defined in § 10–1301(f)(1) of this subtitle, shall provide notice of a breach of security to the Department of Information Technology.

(i) A waiver of any provision of this section is contrary to public policy and is void and unenforceable.

(j) Compliance with this section does not relieve a unit from a duty to comply with any other requirements of federal law relating to the protection and privacy of personal information.

[Previous][Next]